The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
05/16/2017

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in watchOS, iOS, tvOS, macOS, iCloud for Windows, and iTunes for Windows and Safari, the most severe of which could allow for arbitrary code execution. watchOS is the mobile operating system for the Apple Watch and is based on the iOS operating system. iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch. tvOS is an operating system for the fourth-generation Apple TV digital media player. macOS is Apple's desktop and server operating system for Macintosh computers. iCloud is a cloud storage and cloud computing service from Apple. iTunes for Windows is a media player, media library, online radio broadcaster, and mobile device management application developed by Apple. Safari is a web browser available for OS X and Microsoft Windows.

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- watchOS Versions prior to 3.2.2
- iOS Versions prior to 10.3.2
- tvOS Versions prior to 10.2.1
- macOS Versions prior to 10.12.5, 10.11.6 Security Update 2017-002 El Capitan, 10.10.5 Security Update 2017-002 Yosemite
- Safari Versions prior to 10.1.1
- iCloud for Windows Versions prior to 6.2.1
- iTunes for Windows versions prior to 12.6.1

RISK:
Government:

- Large and medium government entities: **High**

- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in watchOS, iOS, tvOS, macOS, iCloud for Windows, and iTunes for Windows, and Safari. The most severe of these vulnerabilities could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- Multiple memory corruption issues were addressed with improved memory handling. (CVE-2017-2494, CVE-2017-2496, CVE-2017-2499, CVE-2017-2503, CVE-2017-2505, CVE-2017-2506, CVE-2017-2512, CVE-2017-2514, CVE-2017-2515, CVE-2017-2519, CVE-2017-2521, CVE-2017-2524, CVE-2017-2525, CVE-2017-2526, CVE-2017-2530, CVE-2017-2531, CVE-2017-2536, CVE-2017-2537, CVE-2017-2538, CVE-2017-2539, CVE-2017-2541, CVE-2017-2542, CVE-2017-2543, CVE-2017-2544, CVE-2017-2545, CVE-2017-2546, CVE-2017-2547, CVE-2017-2548, CVE-2017-6977, CVE-2017-6978, CVE-2017-6979, CVE-2017-6980, CVE-2017-6984, CVE-2017-6985, CVE-2017-6986, CVE-2017-6989)
- Multiple validation issues were addressed with improved input sanitization. (CVE-2017-2502, CVE-2017-2507, CVE-2017-2509, CVE-2017-2516, CVE-2017-2540, CVE-2017-6987, CVE-2017-6990)
- A certificate validation issue existed in EAP-TLS when a certificate changed. This issue was addressed through improved certificate validation. (CVE-2017-6988)
- A certificate validation issue existed in the handling of untrusted certificates. This issue was addressed through improved user handling of trust acceptance. (CVE-2017-2498)
- A denial of service issue was addressed through improved memory handling. (CVE-2017-6982)
- A logic issue existed in frame loading. This issue was addressed with improved state management. (CVE-2017-2549)
- A logic issue existed in the handling of pageshow events. This issue was addressed with improved state management. (CVE-2017-2510)
- A logic issue existed in the handling of WebKit cached frames. This issue was addressed with improved state management. (CVE-2017-2528)
- A logic issue existed in the handling of WebKit container nodes. This issue was addressed with improved state management. (CVE-2017-2508)
- A logic issue existed in the handling of WebKit Editor commands. This issue was addressed with improved state management. (CVE-2017-2504)
- A memory consumption issue was addressed through improved memory handling. (CVE-2017-2527)
- A race condition was addressed through improved locking. (CVE-2017-2501)
- A race condition was addressed with additional filesystem restrictions. (CVE-2017-2533)
- A resource exhaustion issue was addressed through improved input validation. (CVE-2017-2535)
- A URL handling issue was addressed through improved state management. (CVE-2017-2497)
- A use after free issue was addressed through improved memory management. (CVE-2017-2513)

- An access issue was addressed through additional sandbox restrictions. (CVE-2017-2534)
- An inconsistent user interface issue was addressed with improved state management. (CVE-2017-2500, CVE-2017-2511)
- An issue existed within the path validation logic for symlinks. This issue was addressed through improved path sanitization. (CVE-2017-6981)
- An issue in Safari's history menu was addressed through improved memory handling. (CVE-2017-2495)
- Multiple buffer overflow issues were addressed through improved memory handling. (CVE-2017-2518, CVE-2017-2520)
- Multiple memory corruption issues were addressed with improved input validation. (CVE-2017-6983, CVE-2017-6991)

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Apple:
https://support.apple.com/en-us/HT201222
https://support.apple.com/en-us/HT207797
https://support.apple.com/en-us/HT207798
https://support.apple.com/en-us/HT207800
https://support.apple.com/en-us/HT207801
https://support.apple.com/en-us/HT207803
https://support.apple.com/en-us/HT207804
https://support.apple.com/en-us/HT207805

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2494
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2495
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2496
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2497
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2498

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2499
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2500
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2501
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2502
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2503
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2504
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2505
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2506
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2507
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2508
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2509
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2510
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2511
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2512
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2513
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2514
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2515
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2516
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2518
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2519
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2520
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2521
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2524
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2525
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2526
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2527
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2528
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2530
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2531
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2533
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2534
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2535
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2536
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2537
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2538
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2539
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2540
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2541
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2542
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2543
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2544
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2545
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2546
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2547
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2548
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2549
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6977
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6978
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6979
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6980
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6981

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6982
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6983
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6984
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6985
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6986
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6987
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6988
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6989
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6990
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6991